

「国際レベルのセキュリティ組織へ
つながる道」

NSF2022

2022/3/8

自己紹介

- ・ 武井 滋紀 です。
- ・ JNSAのISOG-Jの方から来ました
 - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- ・ NTTテクノクロス株式会社
 - セキュアシステム事業部 アソシエイトエバンジェリスト
 - 2016年度までは社名が「NTTソフトウェア株式会社」でした
 - NTTグループセキュリティプリンシパル
 - ITU-T SG17 WP3 Q3 X.1060 Editor
 - CISSP、情報処理安全確保支援士

ISOG-J とは

- ・ 日本セキュリティオペレーション事業者協議会
 - the Information Security Operation providers Group Japan
 - 2008年創立、2022年3月現在 58組織が加盟
 - プロのセキュリティオペレーター、事業者の集まり
 - 業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です
 - 親団体は日本ネットワークセキュリティ協会(JNSA)
- ・ <http://isog-j.org/>
 - Facebook ページ: /isogj
 - ISOG-J の読み方: いそぐじえい

DXと言われて
セキュリティ対応組織はどうするか？

DXも変化の一つ

変化はDXだけではない

コロナ禍のテレワーク
サプライチェーン
ランサムウェア

GDPR, 改正個人情報保護法

共通する項目

セキュリティは社内システムの一つの問題ではなく、ビジネス全体の問題になった

CSIRTは設立した、でも……

変化に対応できていますか？

5年あれば状況は大幅に変わる

「セキュリティ対応組織(SOC/CSIRT)の教科書 第2.1版

2018年, 第2.1版公開

X.1060により、今、注目されている

X.1060とは

- ・ 2021年6月29日にITU-T(国際電気通信連合の電気通信標準化部門)で国際勧告になった、サイバーリスク対応のための組織のフレームワーク

タイトル：

“Framework for the creation and operation of a cyber defence centre”

「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

配布URL: <https://www.itu.int/rec/T-REC-X.1060-202106-I>

日本語版は？

- ・ 2022年2月に一般社団法人 情報通信技術委員会(TTC)にて、JT-X1060が標準として決定した。
- ・ X.1060が日本での標準として日本語で利用できます。
- ・ 本資料の図表もこちらを引用しています。

タイトル：

「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

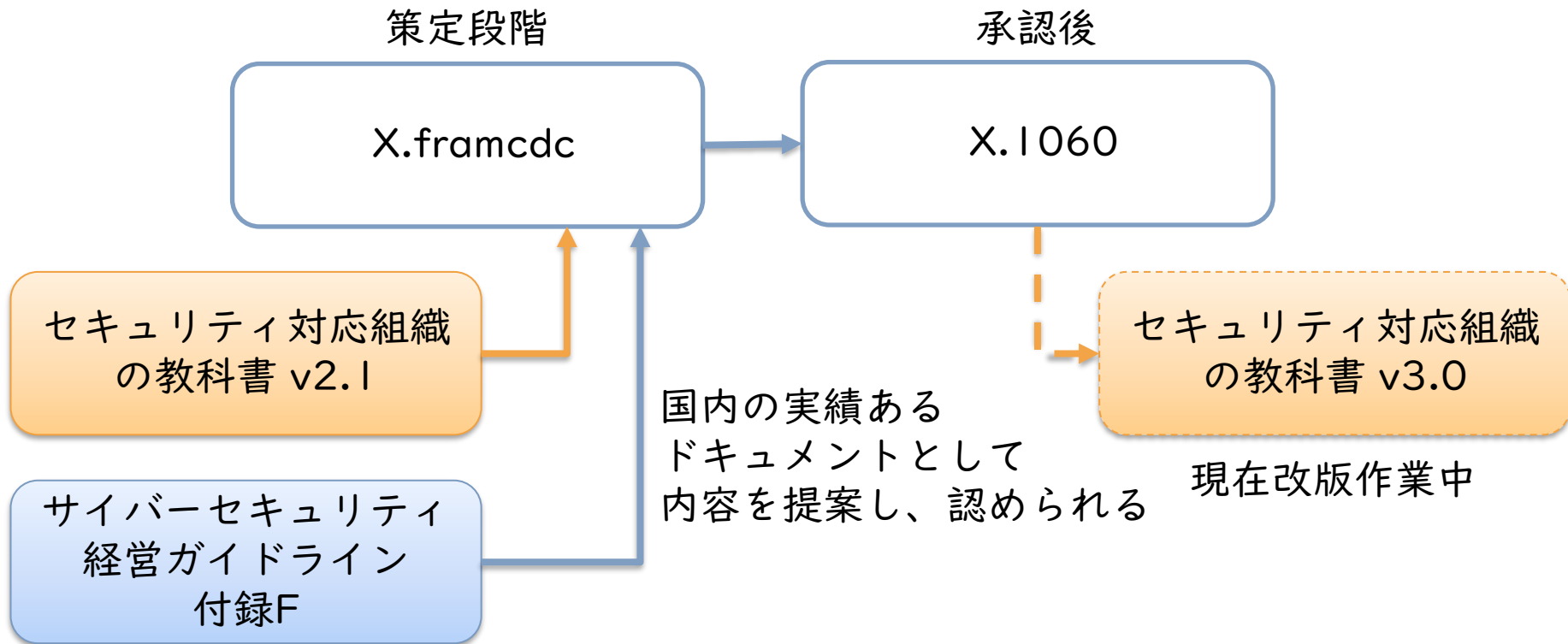
配布URL:

https://www.ttc.or.jp/document_db/information/view_express_entity/1423

X.1060のポイント

- ・ 新しい組織を作るわけではなく、現在のSOCやCSIRTを包含した形
- ・ フレームワークで提示されたセキュリティサービスを実施しているなら、すでにCDCを部分的に構築していると考えられる
- ・ 今後目指す姿として考えていただきたい

X.1060と関連ドキュメントのイメージ



X.1060における組織体制

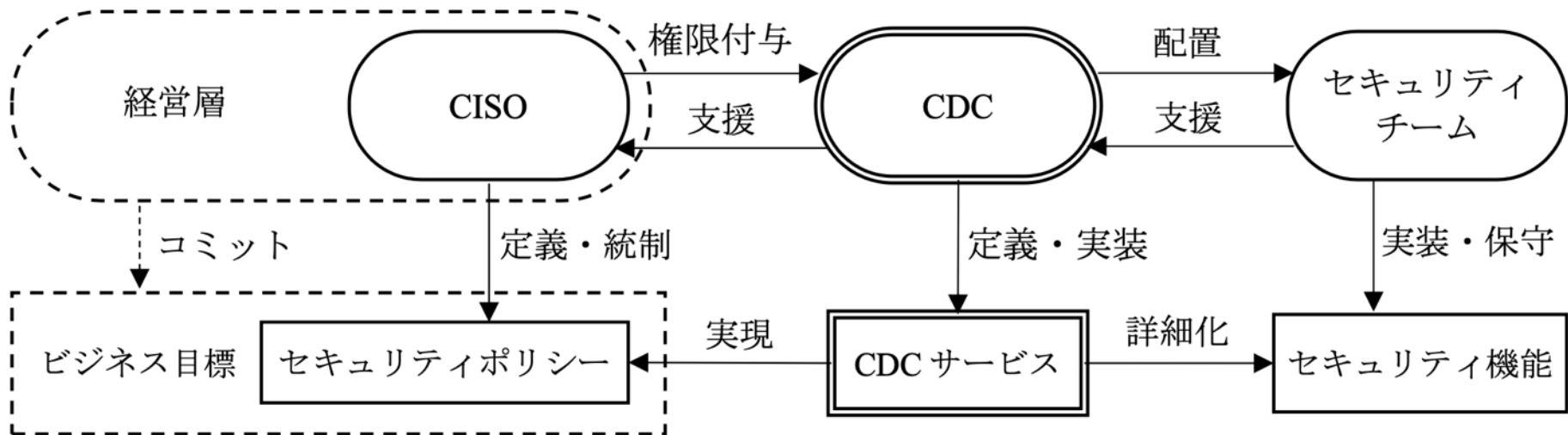


図1 CDCの運営における関係者とその役割

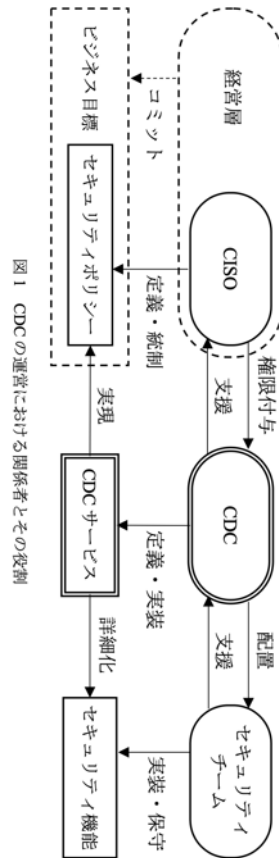
図はJT-X1060より

日本のドキュメントとの比較

サイバーセキュリティ戦略 (NISC)	サイバーセキュリティ経営ガイドライン (METI)	産業横断サイバーセキュリティ人材育成検討会 (CRIC CSF)
経営層 事業継続と新たな価値創出のためのリスクマネジメントの一環として、サイバーセキュリティ対策を推進	経営者 リーダーシップをもってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施。サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）を任命するとともに、経営者自らがリーダーシップを発揮して適切な経営資源の配分を行う。	経営者 (取締役会) セキュリティ統括機能 CISO (経営幹部) 「サイバーセキュリティ統括」機能に責任を負う役割 (役員である必要はない)
戦略マネジメント層 経営戦略等におけるサイバーセキュリティリスクを認識した上で、事業継続と価値創出に係るリスクマネジメントを中心となって変えるとともに、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を擁護し、経営層に報告する役割を担う	10の指示 ↓ 具体的な指示 CISO等 経営陣の一員、もしくは経営トップからその役を任命された、サイバーセキュリティ対策を実施する上での責任者となる担当幹部	セキュリティ統括 (室等) 部門横断的な立場でCISOの役割を担う担当幹部を補佐する部門。 セキュリティの技術的特性を自社の業務に置き換えてリスクを明確化する組織。 基幹となるIT、製造運行等のOT、DXを実現するIoT領域のすべてのセキュリティ戦略に対応。
実務者層・技術者層 戦略マネジメント層が示す概念的・抽象的な考えを理解し、それを具体化するとともに、様々な関係者と円滑なコミュニケーションができる	セキュリティ担当者 ↓ ハンダー企業等	セキュリティ統括担当者 システム部門 担当者 事業部門・管理部門 担当者 セキュリティ統括室長 システム部門 責任者 事業部門・管理部門 責任者 セキュリティ統括担当者 システム部門 担当者 事業部門・管理部門 担当者 セキュリティ専門家 SIハンダー 調達先

図5 セキュリティ統括機能の位置付け (1)

経済産業省 サイバーセキュリティ経営ガイドライン
 付録F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版



各種ドキュメントとの立ち位置

フレームワーク 実践 (どこで、何をするか)

X.1060

経済産業省 サイバーセキュリティ経営ガイドライン 一式

IPA サイバーセキュリティ経営ガイドライン
Ver 2.0 実践のためのプラクティス集

産業横断サイバーセキュリティ検討会
人材定義リファレンス及びスキルマッピング
ユーザ企業のためのセキュリティ統括室 構築・運用キット

日本シーサート協議会(NCA) ドキュメント 一式
CSIRTマテリアル
CSIRT人材の定義と確保

SIM3
Security Incident Management Maturity Model

日本セキュリティオペレーション事業者協議会(ISOG-J) ドキュメント一式
セキュリティ対応組織(SOC/CSIRT)の教科書

セキュリティ対応組織アセスメント

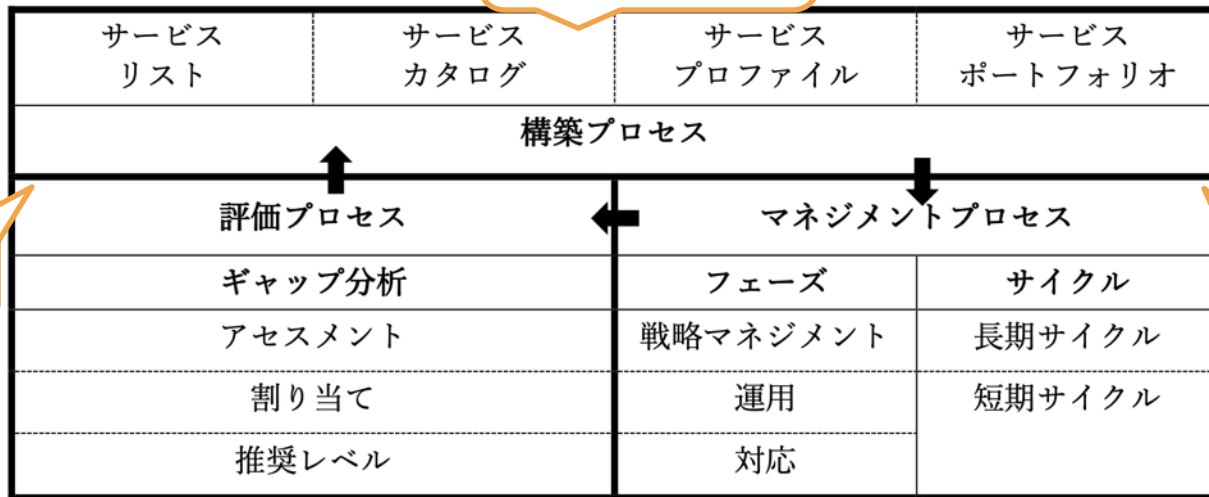
JNSAドキュメント群

CISOハンドブック

SecBok

フレームワーク概要

構築



評価

マネジ
メント

図2 サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

構築プロセス

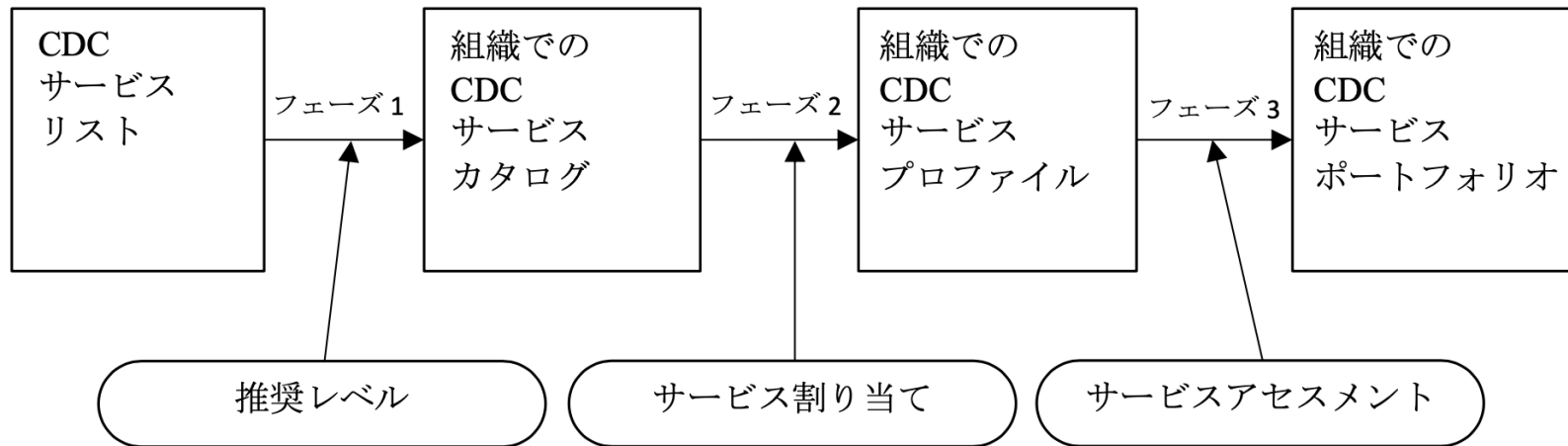


図3 CDCサービスの立ち上げフェーズ

構築は3段階

サービスカタログ

サービスプロファイル

サービスポートフォリオ

図はJT-X1060より

構築は3つのフェーズ

サービスを選ぶ（サービスカタログを作る）

- ・ サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

どこで行うかを決める（サービスプロファイルを作る）

- ・ それぞれのサービスは内製で実施するか、外部委託するか

今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

- ・ それぞれのサービスのスコアをセルフアセスメントで測る

構築プロセス：サービスリスト

X.1060

9つのカテゴリー
64のサービス

ISOG-J

9つのカテゴリー
54のサービス(※)

一覧になれば追加しても良い

※ISOG-Jの教科書もX.1060に合わせて更新します。
☒はJT-X1060より

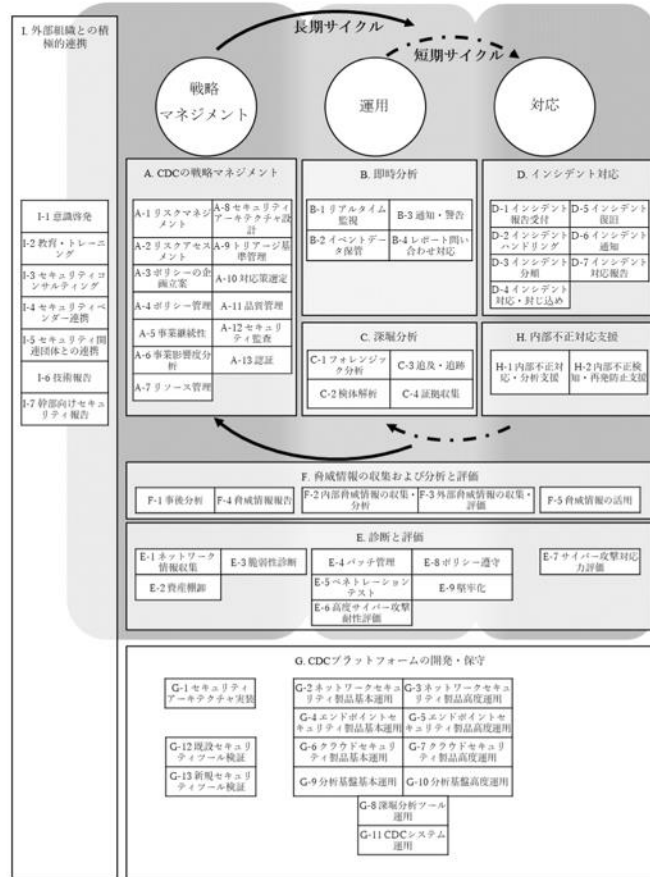


図8 CDCサービスカテゴリー

構築プロセス：サービスのアサイン

X.1060/JT-X1060

ISOG-J

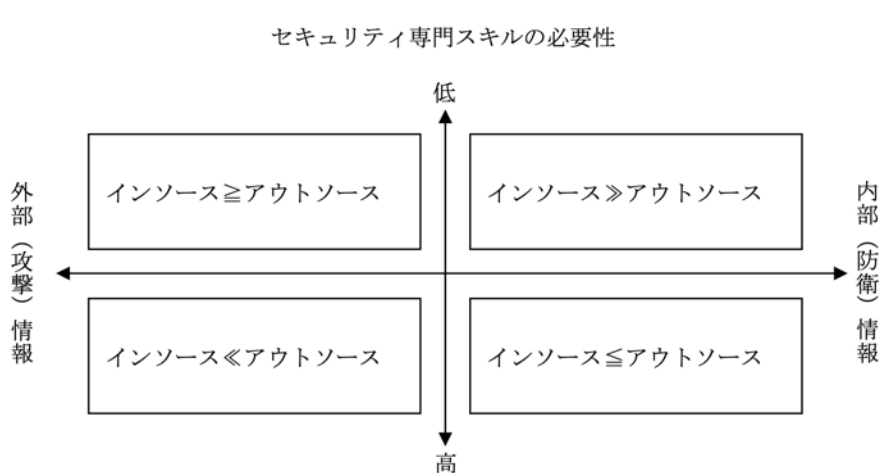


図5 調達の対象

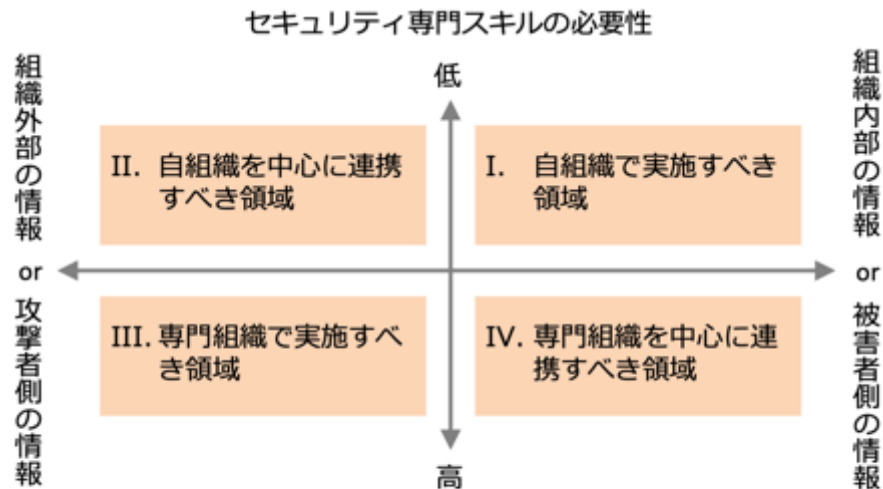


図4 セキュリティ対応の4領域

図はJT-X1060より

構築プロセス：サービスのアセスメント

X.1060/JT-X1060

ISOG-J

表3 CDC サービススコア

インソースの場合	
明文化された運用が CISO など権限ある組織長に承認されている	+5 点
運用が明文化されており、担当者と交代して他者が業務を実施できる	+4 点
運用が明文化されておらず、担当者に代わりて他者が臨時で一部の業務を代行できる	+3 点
運用が明文化されておらず、担当者のみが業務を実施できる	+2 点
実施できていない	+1 点
インソースとしては実施しないと決めた	適用外

アウトソースの場合	
サービス内容と得られる結果を理解でき、想定通り	+5 点
サービス内容と得られる結果を理解できているが、想定未滿	+4 点
サービス内容、得られる結果のいずれかが理解できていない	+3 点
サービス内容と得られる結果を理解できていない	+2 点
結果や報告を確認できていない	+1 点
アウトソースとしては実施しないと決めた	適用外

図はJT-X1060より

- 自組織でその役割を実施する場合（インソース）
 - ・ 明文化された運用は CISO など権限ある組織長に承認されている（+5 点）
 - ・ 運用が明文化されており、担当者と交代して他者が業務を実施できる（+4 点）
 - ・ 運用が明文化されておらず、担当者に代わりて他者が臨時で一部の業務を代行できる（+3 点）
 - ・ 運用が明文化されておらず、担当者が業務を実施できる（+2 点）
 - ・ 実施できていない（+1 点）
 - ・ インソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）
- 専門組織でその役割を実施する場合（アウトソース）
 - ・ サービス内容と得られる結果を理解でき、想定通り（+5 点）
 - ・ サービス内容と得られる結果を理解できているが、想定未滿（+4 点）
 - ・ サービス内容、得られる結果のいずれかが理解できていない（+3 点）
 - ・ サービス内容と得られる結果を理解できていない（+2 点）
 - ・ 結果や報告を確認できていない（+1 点）
 - ・ アウトソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

今後の呼び方は成熟度から変更します。

マネジメントプロセス

日々の改善を実行する
X.1060/JT-X1060 ISOG-J

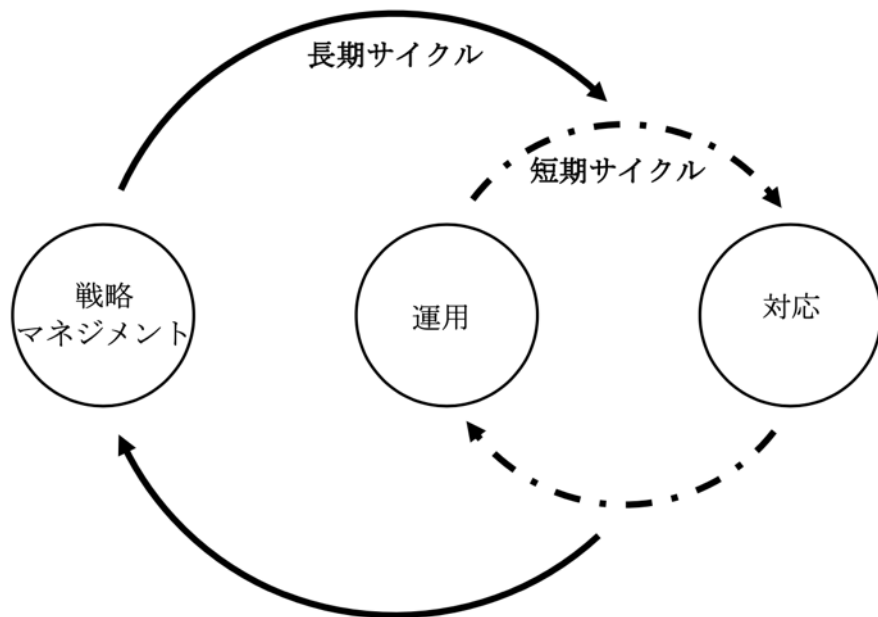


図6 CDC マネジメントプロセス

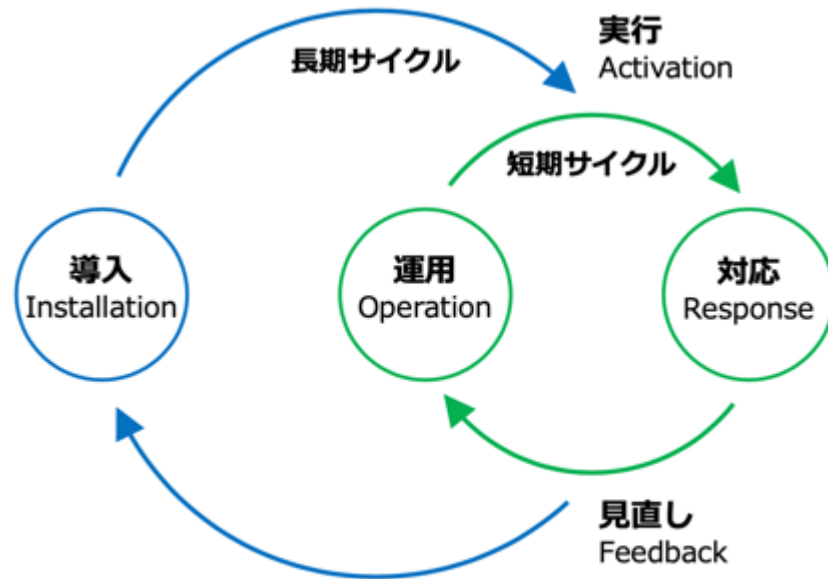
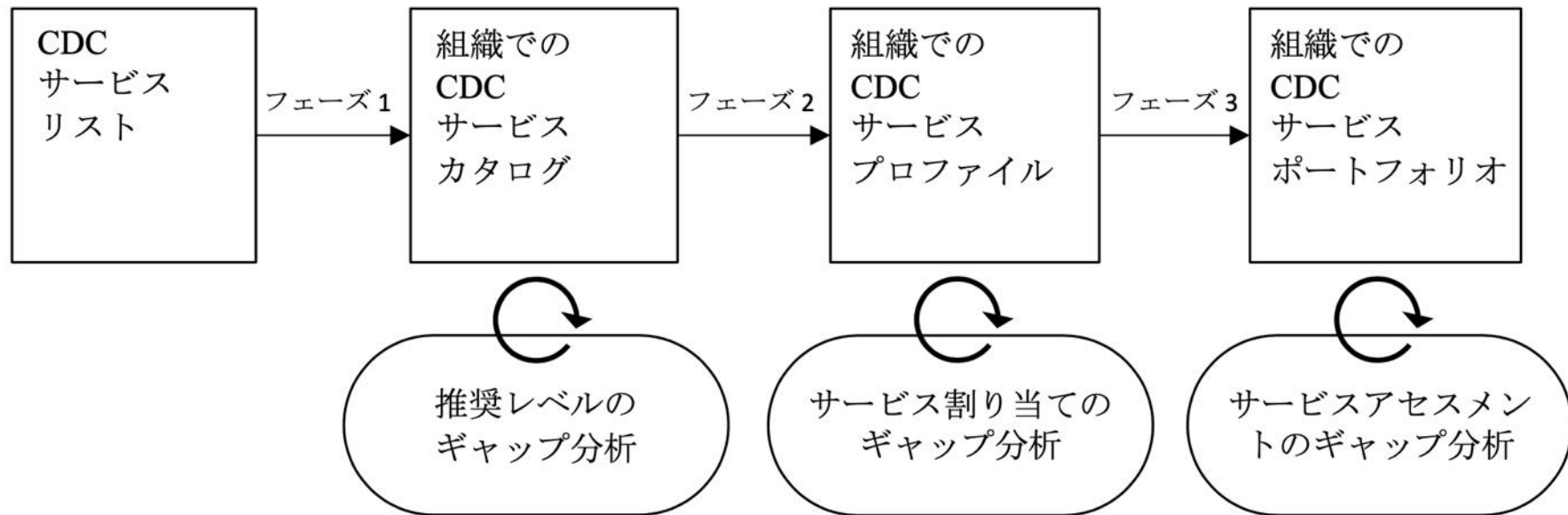


図1 セキュリティ対応実行サイクル

図はJT-X1060より

評価プロセス



図はJT-X1060より

図7 CDC 評価プロセス

構築で行った3つのフェーズそれぞれで見直しをする

評価は構築した3つのフェーズの振り返り

サービスを選ぶ（サービスカタログを作る）

- ・ サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

選んだものは妥当だったか？
状況の変化に対応しているか？

どこで行うかを決める（サービスプロファイルを作る）

- ・ それぞれのサービスは内製で実施するか、外部委託するか

このままで良いか？
割り当てを変えるか？

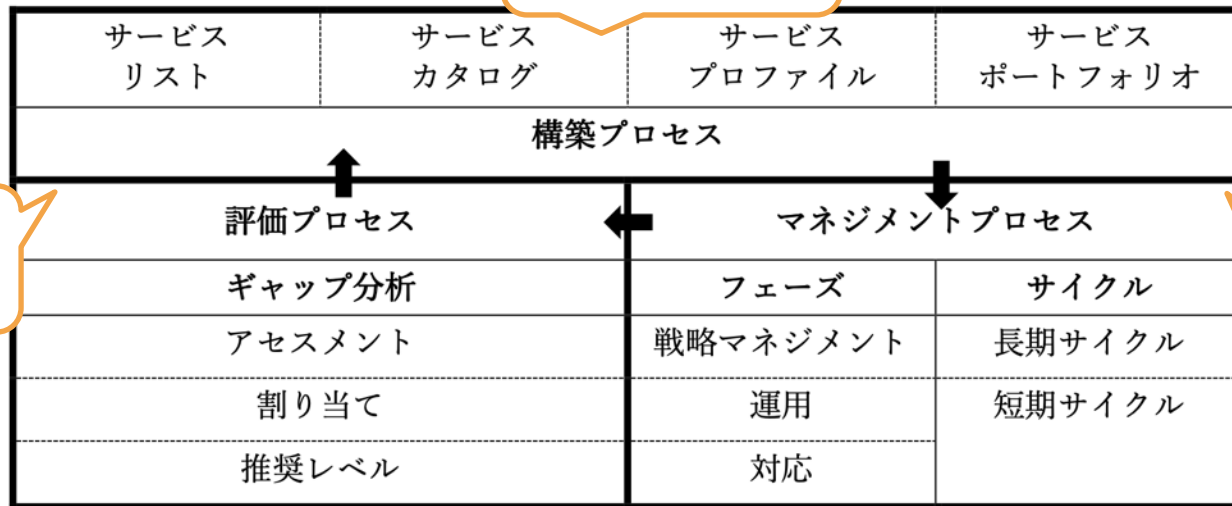
今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

- ・ それぞれのサービスのスコアをセルフアセスメントで測る

今のスコアはどうなった？
目標は変わったか？

フレームワーク概要

構築



評価

マネジ
メント

図2 サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

X.1060の活用

日本のドキュメントも活用

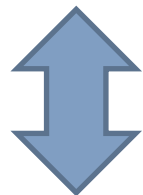
今ある組織のこの先の姿
海外との共通理解として

まとめ

- ・ これからも起こる変化に対応し続けるセキュリティ対応組織が必要となっている
- ・ 継続的な改善を続けるためのフレームワークと、日本語での実用書
- ・ これからも継続的に改善を続けて変化への対応を

X.1060を実現するための参考となるドキュメント群(ISOG-J)

X.1060：国際標準のフレームワーク



具体的な実現方法の参考書

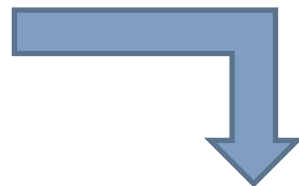
セキュリティ対応組織の教科書

X.1060に対応したv3.0に更新予定



MSSの選び方

マネージドセキュリティサービス選定ガイドライン



情報共有の考え方

セキュリティ対応組織の強化に向けた
サイバーセキュリティ情報共有「5WIH」

ISOG-J ホームページ

<https://isog-j.org>
よりダウンロード可能

セキュリティ対応組織の
教科書も更新を予定して
います

ISOG-J 日本セキュリティオペレーション事業者協議会

日本語 English

日本セキュリティオペレーション事業者協議会 (Information Security Operation providers Group Japan, 略称: ISOG-J) は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進する事業を実施することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に向けて専ら努力することを目的としています。

ISOG-Jについて about us 参加・関連団体 members 活動紹介 activities イベント event information お問い合わせ contact

HOME > 活動紹介 > 活動成果

活動紹介

WGの活動内容
活動成果

活動成果

セキュリティ対応組織の教科書 v2.1 (2018年9月)

2018年9月に、「セキュリティ対応組織の教科書」の概要版となる「ハンドブック v1.0版」と54の役割を一覧できる別紙を追加しております。
2018年3月に、「セキュリティ対応組織成熟度セルフチェックシート」のアウトソースに関する基準を見直したv2.1版に更新しております。

【WG6】セキュリティオペレーション連携WGにおいて、「セキュリティ対応組織の教科書 v1.0」の改版に向けて議論を続けてきました。その中でセキュリティ対応組織に求められる9の機能と、54の役割を、実際のインシデント発生時や平時におけるフローとしてまとめました。また「セキュリティ対応組織成熟度セルフチェックシート」として組織の成熟度をポイント化するツールと合わせて「セキュリティ対応組織の教科書 v2.0」を公開しました(2017年10月 v2.0)。

- 「セキュリティ対応組織の教科書 ハンドブック v1.0」 (PDF形式)
- 「セキュリティ対応組織の教科書 ハンドブック 別紙 v1.0」 (PDF形式)
- 「セキュリティ対応組織成熟度セルフチェックシート」 (Excel形式)
- 「セキュリティ対応組織の教科書 v2.1」 (PDF形式)
- 「セキュリティ対応組織の教科書 別表 v2.0」 (PDF形式)
- フィードバックはこちら(SurveyMonkey)

関連リンク links

JNSA
JPCERT/CC
IPA 情報セキュリティ推進機構
IA japan
WASForum.jp Web Application Security Forum



- ・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
- ・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- ・なお、引用の範囲を超えられる場合もISOG-Jへご相談ください(info (at) isog-j.org まで)。
- ・本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記していません。
- ・ISOG-Jならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。